Compliance & Training Bureau:
Preparing for a Secure Site Audit

Crime Records Division

Non-Criminal Justice: Audit & Training Unit

Ph: 512-424-2474, **option 3** Fax: 512-424-2909

Table of Contents

- **Recent News**
- **Purpose for Audits**
- **Audits**
- **Audit Process**
  - Questionnaire
  - Records Verification
  - Physical Security Inspection
- **Documentation for Audit**
  - Policies and Procedures
  - Encryption Certificates
  - Outsourcing Agreements/Contracts
  - Outsourcing Standard Approvals
- **Who Should Attend Audit?**
- **Contact List**

Recent News
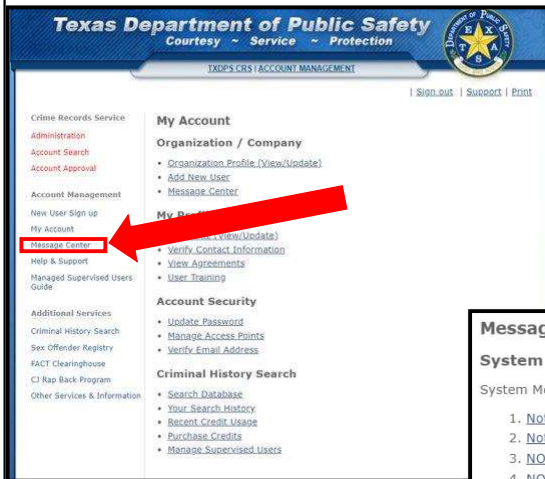
All recent news can be found in your "Message Center"

- Validations
- FBI Name-Based Checks for Fingerprint Rejects
- FRB Subscription Status
- Auto Closing Worklist

Message Center

System Messages

System Messages are messages that are sent to all website users. Select a message to view the message.

1. Notice: Validations Initiated for the TX DPS Secure Site FACT Clearinghouse
2. Notice: FBI Name Check Instructions Update
3. NOTICE: FRB Subscription Status Update
4. NOTICE: New Auto-Closing Worklist Feature

Purpose for Audits

- Ensure agencies are utilizing the Texas DPS Secure Site per their Statutory Authority.

- The objective is to assist agencies in achieving compliance to ensure preparedness for potential audits by the FBI. (Every 3 years)

- Educate and Train Agencies to become Compliant with Criminal Justice Information Services (CJIS) Security Policy and the Access & Dissemination Policy.

- Ensure Criminal History Record Information (CHRI) from the Secure Site is secured both electronically and physically.

- Educate and Train agencies to use the FACT Clearinghouse and/or the Criminal History Search Services more efficiently.

Audits

- **<u>Non-Criminal Justice</u>** Audits pertain to the administration and operation of the FBI Rap Back program in the FACT Clearinghouse, as well as the Computerized Criminal History Search service.
- The Texas Department of Public Safety and Federal Bureau of Investigation perform routine audits on non-criminal justice accounts **<u>every three years.</u>**
- **2 Types of DPS audits:**
  - Onsite Audit
  - Electronic Audit (Microsoft Teams Meeting).
- **Who Should Attend Onsite Audit?**
  - Account Supervisor for Secure Site
  - Data Users (optional)
  - IT personnel (optional)
  - If needed, you may include individuals who make the decisions for the agency. (example: (Chief, Sheriff, Captain, Investigator)

Audit Process: Confirmation Letter

Texas Department of Public Safety
Crime Records Division
Compliance & Training Bureau

Agency Audit Confirmation

Agency Name: OrgID:

Date of Audit: Time of Arrival:

Agency Person of Contact Name:

Physical Address:

Purpose of Audit:

The *Compliance & Training Bureau* is required to conduct security audits of each agency with access to criminal history records information from the Secure Site, every three (3) years at a minimum. This is to determine compliance with the *Access & Dissemination Policy* and the *CJIS Security Policy*.

Prior to the onsite audit, an electronic audit questionnaire and verification of records will be assigned to your agency to respond within seven (7) business days.

On the date of the onsite audit, an administrative interview is conducted with appropriate agency personnel. Following the interview, the auditor will perform a physical security inspection, which involves a tour of the facility, including anywhere the agency is processing, storing, or accessing CJI and records verifications.

I understand the purpose of the audit and confirm to be available for the audit.

Agency Person of Contact Signature   Date

ADB Auditor   Date

Phone: 512-424-2474, option 3 Fax: 512-424-2909

Onsite Audit

Virtual Audit (Microsoft Teams)

It all starts with contact from an Auditor, they will let you know if it is an onsite audit or electronic

We will try to work with your schedule to schedule the audit.

Audits are not optional FBI/DPS makes them a requirement this is stated in the agreements your agency signed when you opened the account.

You will sign the confirmation letter and return it to your auditor.

During the electronic audit process the auditor will schedule a Microsoft teams meeting to go over the audit findings.

Audit Process: Questionnaire

- The first step of the audit process is the CJIS audit questionnaire, this offers auditors valuable insight into the training needs of the agency, as well as any compliance issues that require attention.

- This questionnaire will be reviewed during the onsite visit or the scheduled Microsoft Teams meeting. The questionnaire includes a multitude of topics some which might not all apply to your agency. Answer the questionnaire to best of your abilities it is acceptable to answer with "I do not know" or "unsure". <mark>THIS IS NOT A TEST, THERE IS NO PASS OR FAIL</mark>

- After the meeting you will be required to log back into the CJIS audit questionnaire portal to provide a plan to rectify any non-compliance items, change your answers or to acknowledge any information the auditor provides.

Documentation: Policies and Procedures

Auditors will request a copy of the agency's Policies and Procedures addressing the following:

- **Policy for CJIS violators.** (CJIS Security Policy 5.12.4)
- **Physical protection policy to ensure the security of CHRI.** (CJIS Security Policy 5.9)
- **Protection and procedures policy for electronic and physical media.** (CJIS Security Policy 5.8)
- **Policy and procedures for the sanitization and destruction of electronic media.** (CJIS Security Policy 5.8.3)
- **Policy for the disposal and destruction of physical media.** (CJIS Security Policy 5.8.4)
- **Incident response policy.** (CJIS Security Policy 5.3 and 5.13.5)

Sample policy is available in the DPS CJIS Launchpad.

Audit Documentation: Encryption Certificates

- **If the agency's legislative authority allows CHRI to be stored electronically, the auditor will request a copy of the Encryption Certificates for the following:**
  - Electronic Database
  - Email Server
  - Cloud Server
- **Encryption Certificates must be FIPS140-2/197 as required by the CJIS security policy.**
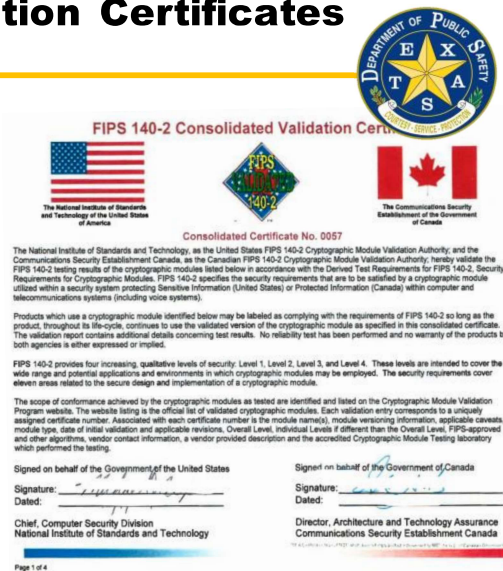
Audit Documentation: Outsourcing Agreements/Contracts (Non-CJ Agencies)

- **Outsourcing Agreements/Contracts for the following third-party vendors who will view or assist with CHRI:**
  - Data Destruction (paper shredding, hard drives, etc.)
  - IT Services (network/system administrators, desktop support, etc.)
  - Off-site Media Storage (data centers, backup, paper storage archives etc.)
  - Hiring Decisions (mail offer letters, generates security badges/credentials, etc.)
  - Scanning Services (scan results into database or electronic file)
- **<u>Depending on the services, an Outsourcing Standard can be prevented if authorized personnel from the agency performs or witness the services.</u>**

Audit Documentation: Outsourcing Standard Approvals (Non-CJ Agencies)

- **All outsourced vendors will have to be vetted through TX DPS and become CJIS Security Policy approved.**
- **The following will need to be in place for an Outsourcing Standard:**
  - Written Request Letter.
  - Copy of the contract with the vendor. It must reference the CJIS Security Policy and Outsourcing Standard Agreement.
  - A completed Outsourcing Standard.
- **After outsource vendors are approved, agency will have to:**
  - Conduct an audit within 90 days of the Outsourcing Standard Agreement approval date.
  - Report any incidents to TX DPS.
  - Keep vendors current with CJIS Security Policy.
  - **Vendors are required to complete CJIS security awareness training and be fingerprinted** (If statute permits)

Audit Documentation: Outsourcing Agreements/Contracts (CJ Agencies)

- **Security Addendum or Management Control Agreement for the following third-party vendors who will view or assist with CHRI:**
    - Data Destruction (paper shredding, hard drives, etc.)
    - IT Services (network/system administrators, desktop support, etc.)
    - Off-site Media Storage (data centers, backup, paper storage archives etc.)
    - Hiring Decisions (mail offer letters, generates security badges/credentials, etc.)
    - Scanning Services (scan results into database or electronic file)

Audit Documentation:
Outsourcing Agreements/Contracts (CJ Agencies)

- **Security Addendum or Management Control Agreement Required (IT, Storage, Data Destruction, and Retrieval)**
  - Samples available in CJIS Launchpad
  - Management Control Agreement for Governmental Non-Criminal Justice Agency providing the service - Ex: City/County (CJIS 5.1.1.4)
  - Private vendors/contractors require Security Addendum (CJIS 5.1.1.5)
- **Vendors are required to complete CJIS security awareness training and be fingerprinted**

Audit Process: Records Verification

Onsite Audit

- **Prior to the Onsite Audit, the Auditor will send a list of records to be verified.**
  - The agency will complete the list and return to their auditor within 7 business days via email.
  - During the audit, the agency will be asked to provide documentary evidence for each record on the list, to validate the purpose of search.

Electronic Audit

- **In the electronic audit process, the list of records will be sent at the initial process of the audit.**
  - The agency will be requested to return the completed records verification list, <u>along with the supporting documentation to verify each search record</u>, via email within seven business days.

Audit Process: Records Verification

You will receive something similar to this in our records verification process.

Top: will ask you for the detailed reason for search please be specific ex: Applicant for employment: attendant, driver, officer, teacher

Bottom: will ask you the same question with an additional separation date, if the individual is currently employed or licensed leave blank if they have been separated from your agency give an approximate date.

Audit Process: Records Verification (CCH Searches)

To prepare for the audit make sure you have each one of your searches logged and have some sort of documentation to proof purpose.
Ex: Job applications, payroll, job offer

Audit Process: Records Verification (FACT Searches)

Offline Applicant Management = Full subscription list

To prepare for our audit you should download your full list of employees and make sure they are all current employees, here is how you do it.

Audit Process: Records Verification (FACT Searches)

SID	ORI	OCA	NAM	DOB	VAL	HasTexasSubscription	FRB Subscription Status	FP Date	SSN	Validate/Cancel
0	TXSAMPLE		Doe, John	1975-04-06	2021-08-09	Y	SUBSCRIBED	8/4/2021 10:58:41 AM	0	?V/C
0	TXSAMPLE		Doe, Jane	1965-05-07	2023-07-03	Y	NOT ELIGIBLE	11/5/2012 12:06:43 PM	0	?V/C
0	TXSAMPLE		Hungry, Hippo	1967-12-27	2021-09-07	Y	ELIGIBLE		0	?V/C
0	TXSAMPLE		Gator, Investigato	1960-02-03	2022-08-02	Y	PENDING		0	?V/C

Column Name	Description
SID	State identifier - a number assigned to that specific individual.
ORI	The organization the individual was printed for, and what your agency is using to subscribe to the individual/access their criminal history.
OCA	Miscellaneous number that is different for each agency. This is an optional field.
NAM	The individual's name.
DOB	The individual's date of birth.
VAL	The date the record was last validated. Note this is not always the same as the fingerprint date.
HasTexasSubscription	Shows if you are currently subscribed to the applicant's Texas record (Y/N).
FRB Subscription Status	Shows if the individual's SID is eligible for FBI Rap Back OR their current status. This is based on the most recent submission for the ORI selected to create the subscription. More details on the FBI Rap Back columns in the list can be found in the section FBI Rap Back and the Applicant List.
FP Date	The date the individual was last fingerprinted *for the ORI selected for the subscription.*
SSN	The individual's Social Security Number.

Search FACT Clearinghouse

- View Worklists

Applicant Search

Read Me

You can search for applicants directly associated with your organization or for applicants in the FACT Clearinghouse that are indirectly associated with your organization.

Once an applicant has been found, you may review their Consolidated Response and then optionally subscribe to their record.

If you are unable to locate an applicant, they may not be part of FACT Clearinghouse or may be under a different name or not accessible to your agency.

SID Search

Notes

The SID is a unique ID assigned by DPS. If you know this value, this is the best method for locating an applicant.

SID (Required)

Search

You should receive an excel sheet like the one pictured on the top and you can use this to manage subscriptions and unsubscribe to individuals you are no longer associated with.
Subscribed
Not Eligible
Eligible
Pending

Audit Process: Records Verification (FACT Searches)

You must ensure you do this 3 business days after separation from your agency to stay in compliance.
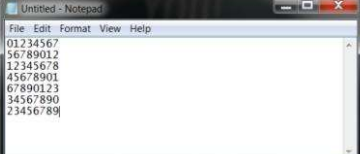
Audit Process: Records Verification (FACT Searches)

Open a basic text editor like Notepad.
  a. Notepad is included with all Windows systems and can usually be found under the Accessories folder in the Start Menu.
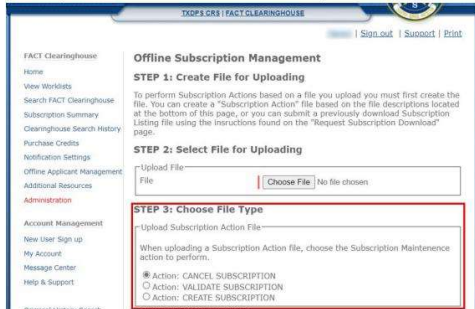Copy the SID for each of the applicants you want to cancel OR validate and paste them into Notepad.
  b. **Do NOT put SIDs to cancel and SIDs to validate on the same list.**
  b. Ensure there are no spaces, tabs, or extra returns. The file will not upload correctly if there is anything other than 8-digit SID numbers followed immediately by a return to the next line.
Save the file to your computer. The file name does not matter, however it is recommended to include the list purpose e.g. SIDs_to_Validate.

Untitled - Notepad
File Edit Format View Help
01234567
56789012
12345678
45678901
67890123
34567890
23456789

Select the action you wish to perform.
  a. Cancel Subscription – Will disable/cancel all subscriptions on the uploaded file.
  b. Validate Subscription – Will validate all subscriptions on the uploaded file.
  c. Create Subscription – Will create subscriptions to all individuals on the uploaded file. NOTE: This will require an ORI be included for each SID number uploaded.

TXDPS CRS | FACT CLEARINGHOUSE
| Sign out | Support | Print

FACT Clearinghouse
Home
View Worklists
Search FACT Clearinghouse
Subscription Summary
Clearinghouse Search History
Purchase Credits
Notification Settings
Offline Applicant Management
Additional Resources
Administration

Account Management
New User Sign up
My Account
Message Center
Help & Support

Criminal History Search

Offline Subscription Management

STEP 1: Create File for Uploading

To perform Subscription Actions based on a file you upload you must first create the file. You can create a "Subscription Action" file based on the file descriptions located at the bottom of this page, or you can submit a previously download Subscription Listing file using the instructions found on the "Request Subscription Download" page.

STEP 2: Select File for Uploading

Upload File
File   [Choose File] No file chosen

STEP 3: Choose File Type

Upload Subscription Action File

When uploading a Subscription Action file, choose the Subscription Maintenence action to perform.

◉ Action: CANCEL SUBSCRIPTION
○ Action: VALIDATE SUBSCRIPTION
○ Action: CREATE SUBSCRIPTION

You must ensure you do this 3 business days after separation from your agency to stay in compliance.

Audit Process: Physical Security Inspection

Onsite Audits

- Auditors will inspect the following:
  - Ensure areas where CHRI is processed are secured.
  - Ensure that monitors are secured from unauthorized viewing.
    - If they can not be faced away from unauthorized viewing, a privacy screen must be in place.
  - Ensure password to Secure Site is secured. (Do Not Auto-Save/ Auto-Fill Password)
  - Ensure a session Lock in place for computers (30 mins or less).
  - Ensure that network servers are locked in secure room or closet.

- After Onsite inspections have concluded, the auditor can assist and train your agency. They will be available for any questions or concerns.

Electronic Audits

- Electronic audits will require photos of secured areas to be submitted prior to the virtual meeting.

- During the Microsoft Teams meeting, the auditor will discuss findings and will provide training to address any questions or concerns. They may also ask you to share your screen or provide additional documentation

Audit Documentation: DPS folder

- **We recommend having a folder or binder with the following:**
  - A copy of your legislative or federal authority
  - SOP's: Detail what you do daily on the secure site and more importantly what you do not do. If you store CHRI outline how you store, how long you store and who has access to the stored CHRI.
  - Agency Policies and Incident reporting form: Samples Available in the CJIS launch pad
  - Link to the Access and Dissemination policy, this contains the link to CJIS security policy.
  - Tracking Logs (CCH Name Based Searches)
  - NCJU Audit Packet (CJIS Launch Pad)
  - Encryption Certificates

Resources

- **Non Criminal Justice** CJIS Launch Pad:
    - **https://texas.cjisapps.com/noncrim/launchpad**

- **Access & Dissemination Policy:**
    - **https://securesite.dps.texas.gov/DpsWebsite/CriminalHistory/SecurityPolicy.aspx**

- **Crime Records General Information:**
    - https://www.dps.texas.gov/section/crime-records/crime-records-general-information

Public Resources

- **DPS Public Site:** Convictions or deferred adjudications that have been reported to the Department on an offense.
  - https://publicsite.dps.texas.gov/convictionnamesearch/
- **DPS Public SOR**:
  - https://publicsite.dpd.texas.gov/sexoffenderregistry/
- **TXI Review/ TXE Review**
  - dps.texas.gov/internetforms/Forms/CR-63.pdf
  - dps.texas.gov/internetforms/Forms/CR-68.pdf

If your legislative authority does not let you run a specific population, we have option on the public records side of DPS.

Contacts

Criminal History Inquiry Unit

Email: NCJU@dps.texas.gov

Phone: 512-424-2474, option 1 & 2

Audit and Training Unit

Email: CJIS.Audit@dps.texas.gov

Phone: 512-424-2474, option 3

Billing Unit

Email: CRS.Billing@dps.texas.gov

Phone: 512-424-2474, option 4

ADB Support Unit

Email: ADBSUPPORT@dps.texas.gov

Phone: 512-424-2474, option 5

Fingerprint Services Unit

Email: Fingerprint.Service@dps.texas.gov

Phone: 512-424-2365, option 6

Please fill out our survey!

Preparing for a Secure Site Audit (Non-Criminal Justice Unit) -
https://www.surveymonkey.com/r/2BCG5ML

- Carlos Ramirez